ATOMICdata

OUR APPROACH TO

SECURITY & COMPLIANCE

The safety and security of your data is our highest priority. Atomic Data implements best-practice systems, procedures, safeguards, and attestations to protect client data from unauthorized access or disclosure. Combined with our expert engineers and enterprise-grade infrastructure, Atomic Data provides clients with safe, simple, and smart solutions.

Some of the steps we take to safeguard client systems and data include:

- **SOC 2 Type II attestation.** Atomic Data systems meet industry standard requirements in regards to controls over security, availability, and confidentiality.
  - Externally audited & attested since 2011 in accordance with AICPA standards
  - Assesses Security, Availability, & Confidentiality controls
  - View the report at atomicdata.com/soc
- **Management and oversight.** From our Executives and Advisory Boards all the way down to our Technicians, security and compliance are always top of mind.
  - Enterprise Governance Board oversees control environment and reviews/approves changes
  - Internal Security & Compliance identifies, monitors, evaluates, & mitigates risks
  - Internal Security & Compliance is responsible for the operation, maintenance, & improvement of Atomic Data's control environment
- **Policies and procedures.** We adhere to a written set of policies and procedures that address risk assessments, change management, access, education, and much more.
  - Change & Risk Management policies
  - Event Management System for planned maintenance, unexpected events, exceptions
  - Mandatory Security Awareness training
  - Annual criminal background checks
- **Access controls** at the logical and physical layers ensure that data, platforms, and hardware are only accessible to those people or systems that require it and are approved to do so.
  - Dual-factor, audited cage locks
  - 24x7 monitoring & on-site security
  - Video surveillance, door sensors, biometrics, multi-factor security, background checks, etc.
  - Unique identifiers for each user, zero-trust principles
  - Authentication using: unique tokens, card key, biometric reader, or individual passwords
  - Complex passwords, MFA mandated
- **Computing, software, and network controls** keep Atomic Data's infrastructure and your data segregated, protected, encrypted, patched, tested, and monitored.
  - Physical/logical network isolation
  - Cisco enterprise firewalls & F5 IPS & IDS
  - Data traverses through encrypted channels (IPSEC VPN, SFTP, SSL, HTTPS, MPLS)
  - Vulnerability scanning & 3rd party pen testing
  - Code review & patching follow best practices
  - Configuration hardening
- **Data destruction and disposal techniques** further ensure that no matter the medium, your sensitive data won't fall into the wrong hands.
  - Data purging via degaussing & secure overwriting
  - Physical destruction via shredding, burning, disintegration, etc.
  - All data disposal is documented